

## **Chapter Nine**

### **Intelligence and Force Protection vs Terrorism**

*Peter S. Probst*

I think most recognize that the world as we know it is in a state of flux and transition due, in large part, to the disintegration of the Soviet Union and the end of the Cold War. Economic forces, resurgent nationalism, militant Islam, linguistic and cultural differences, rampant corruption, coupled with actions of ruthless demagogues, have contributed in varying degrees to the chaotic conditions we now see in the former Soviet Union, the Balkans and, unfortunately, in too many other countries and regions of the world.

Radical Islam is a potent force in much of the Middle East, the Muslim ghettos of Europe, and is evidenced here in the United States as well. Violent Islamic extremists with deep pockets, such as Osama bin Laden, have developed a global reach and are working relentlessly to procure weapons of mass destruction.

An emerging and significant threat is represented by improvised biological, chemical and nuclear devices that exploit technologies that once were the sole preserve of world and regional powers. The ability to decimate large population centers and wreak havoc on an unprecedented scale has devolved from nation-states to groups and now even to the individual.

The possibility of a biological Unabomber armed with pulmonary anthrax or plague is a reality as near as tomorrow's headlines. Whether they be nations or lone individuals, proliferation enables those who are traditionally at the margins to play a major role on the world stage. Improvised weapons of mass destruction will be the great equalizers of tomorrow, providing the means for the disaffected and deranged to directly impact on the core interests of world powers.

The world as we know it is forever changed. Our strategies, tactics, and capabilities need to reflect these new realities if we are to successfully

meet the terrorist challenges of the post-Cold War era and successfully navigate the treacherous waters of this “brave new world” which our children will ultimately inherit.

To be effective, intelligence and antiterrorism must be inexorably linked. They are two sides of the same coin and must engage in a continual interactive and iterative process in which existing antiterrorism standards, tactics, doctrine, and training are continually measured against the latest intelligence and anticipated developments so that our approach may be adjusted accordingly. We cannot have effective antiterrorism without effective intelligence collection and analysis.

Nor can we have effective antiterrorism if we base our security on the demonstrated capabilities of our terrorist adversaries. To do so, in effect, is to plan for yesterday’s attack; and we will be blindsided when terrorists adopt new tactics or significantly increase the lethality of their current arsenal.

Currently, many in our community are focusing on terrorist use of improvised weapons of mass destruction. There can be little doubt that such weapons could have devastating results. I fear, however, our preoccupation with the exotic is causing us to focus less on the mundane. And this has me concerned.

One tactical approach for which we are unprepared is terrorist exploitation of the Third Country Nationals (TCNs) who work at our overseas installations. They may work in food service, or as members of the charforce, or in the BX. These are the invisible people. These are the people we rarely notice, but their work gives them access to the food, water, medicine, and other consumables used by our troops.

Another example of a potential insider threat is our use of foreign contractors about whom we know too little. Our continued use of the bin Laden construction company and its affiliates on construction projects at some of our most sensitive installations in the Gulf is a case in point. The opportunities for a member of the construction crew to do serious mischief should not be underestimated and can be very difficult to detect. Moreover,

implantation of devices need not take place on site if access to the materiel can be obtained during manufacture or transport. The security implications are obvious. How we will deal with them is problematic.

All this being said, the fact remains that the emphasis of such programs is “after the fact”—after an individual has been observed acting suspiciously, or after a suspicious incident has occurred. A trained terrorist operative is unlikely to attract attention. Such an individual need only act once and, most likely, his actions would appear to be within the norm.

Awareness programs, although extremely important, are largely reactive in nature. They depend on the good guys spotting someone committing a bad act—an action that is out of character and, therefore, inherently suspicious. These programs are important, but they address only one aspect of the problem.

To be truly effective security programs must be primarily proactive. Programs must be in place to prevent potential miscreants from obtaining access to vulnerable and vital DoD installations in the first place. In other words, through intelligence, we must vet those who are in positions to do us harm. If we cannot provide ourselves such assurances, then we cannot afford to employ them. The potential risk is too great. It is only common sense. This is the role of antiterrorism/force protection through intelligence. This should be the heart of our security program and, as far as I can determine, is not being adequately addressed, if addressed at all.

The arguments against such an approach generally boil down to monetary considerations. It would cost too much. It would mean either American soldiers or contract labor that can be vetted would be used, and the costs could be exorbitant.

Yes, it would cost more but how much are the lives of American soldiers worth? What is the price tag we put on our country’s security interests? The irony is that if TCNs were involved in some future Khobar Towers type attack, such policy changes would be made overnight. And

regrettably, after the fact. My view is, why wait? Why risk more tragedy and trauma, and more heartbreaking ceremonies at Dover AFB.

For those concerned about the bottom line—and let's be realistic, we all are—such costs would likely be greater because the changes would be implemented rapidly—probably by fiat and without adequate study. Other costs cannot be calculated. These are the costs of American lives and prestige. Such losses have no price tag.

In order to be truly effective I think antiterrorism must be viewed in the broadest sense. If we commit ourselves to a static defense, we will be constantly probed and tested until a weakness is found and our defenses penetrated. To put it less delicately, a bunker mentality will get you killed.

One possible fix is to extend our effective perimeter beyond the installation gate by developing ties with surrounding villages and towns. It is the traditional hearts and minds approach, and it still has validity today.

For example our engineers can build roads that enable those in villages near our bases to bring their goods to market, and link remote towns and villages to the capital. Roads are the arteries that bind remote and isolated populations together as an interdependent political and economic entity we call a nation. Roads promote a sense of nationhood and a mutuality of interests. Roads also enable the military to more rapidly reach isolated areas to assist in mitigating natural disasters and to provide requisite security.

Bringing radio and television to such areas also is extremely constructive. These media can provide health, farming, literacy, and other educational programming to better the lot of local inhabitants. Our engineers can also repair bridges, build schools, dig wells, and run pipe to provide potable water. These activities not only raise the standard of living, but create links between our troops and the local population. Gradually our perceptions of the locals change and so do theirs, as genuine friendships and loyalties develop.

Where security and custom permit, troops can also become involved in off-duty activities such as coaching kid's soccer, teaching in local schools, or assisting in orphanages and hospitals.

One of the most valuable tools is the use of mobile medical teams that minister on a regular basis to the local population. Such activities promote trust and confidence. They also can serve as a trip wire by providing a channel for local villagers to report events or developments that they fear may impact on their security or well-being.

I like to view antiterrorism as a series of concentric circles, the common denominator being intelligence. Our aim should be to extend these perimeters to the maximum.

Use of an active defense provides additional layers of security. But I would like to expand the concept. I firmly believe the best defense is an aggressive offense in which traditional counterterrorism, antiterrorism, intelligence collection, and covert action are seamless and integrated.

Even our best-guarded bases are not islands unto themselves, but very much tied to the outside world. Our bases have numerous portals of entry besides the front gate. And these other avenues of access also need to be guarded and secured.

For example, is our installation dependent on a local pipeline and pumping stations for water? Contrary to what many believe, water, when supplied in this fashion, may be successfully contaminated with several commercially available and very lethal agents. If our drinking water is delivered by tanker truck or stored in large bladders the terrorist's job may be even easier, particularly if the bladders are not adequately secured.

Local procurement or transport of food stuffs offer similar opportunities. Our veterinary officers may make random checks for conventional risks such as spoilage but, for the most part, they are neither trained nor have the means to detect poisons or other contaminants that may be purposely introduced.

In many respects, the greatest challenge we face is not the terrorist's access to technologies of mass destruction. Nor is it his ability to employ computers and the Internet to enhance his security, develop and exploit information, and extend his operational reach. Nor is it even his increased sophistication in waging war in the political arena.

In my view, the greatest threat to our security remains problems of mindset and perception. We fail to appreciate how phenomena such as mindset and perception impact on terrorist thinking and operations. Further, we rarely consider how such phenomena constrain and distort our own views and premises on which we base our operational planning.

Failure to identify and understand our own mindset may cause us to overlook or dismiss potentially catastrophic vulnerabilities and, at the same time, constrain our ability to fully exploit those of our terrorist adversaries.

Whether an individual or a nation, the perceptions one holds molds the reality in which one operates, and the methods and means one develops to navigate in that reality. For all practical purposes, "perception is reality." Or to put it somewhat differently "reality is in the eye of the beholder." If we are to defeat our terrorist adversary, we must understand his "reality" and how he adapts to it and operates in it. This remains one of our major intelligence gaps.

We need to understand on a group-specific basis how the terrorists think, how they plan, how they collect intelligence, select targets, weigh options, and adapt to operational adversity.

From the antiterrorism standpoint, we also need to understand how the terrorists view us and our security measures. What do they see as our strengths, weaknesses, and levers to be manipulated? In other words, we need to see ourselves and our security measures, through the eyes of our terrorist adversaries. Then, when there is no hard intelligence as to the venue or timing of the next attack, we can more intelligently game out the terrorists available options and how the terrorist will most likely play his hand.

The terrorists' perceptions—right or wrong, accurate or inaccurate—will drive their strategy, tactics, and planning. An understanding of such

factors is one key to developing an effective antiterrorism program. Conversely, our own perceptual lenses colored by culture, history, personal experience, and bureaucracy may further distort an already flawed or incomplete picture.

If the past is any predictor of the future, in most instances we will not obtain the intelligence necessary to pre-empt terrorist operations. And that is the rub. If it is unlikely we will be able to detect, deter, or preempt a significant number of terrorist attacks, we then need to change the rules of the game and modify the “reality” in which the terrorist operates.

What I am talking about is developing information and analysis that enables us to better predict how, when, and where the terrorists will strike because we have fed them the information on which they will likely act. In other words, we need to develop an exceedingly robust deception, disinformation, and covert action capability. What I am advocating is an orchestrated, group-specific campaign to confuse and confound the enemy, and cause him to squander resources, take unwise risks, force his hand, and entice or propel him to commit operational blunders.

Through careful analysis we can develop a better understanding of how a particular terrorist group is likely to process information, what factors are given particular weight, and the operational predilections of the terrorist leader and his planners.

Targets that are lucrative and essentially undefendable can be made to appear “hardened.” Seemingly lucrative and vulnerable targets that, in reality, are traps waiting to be sprung may be created—their value and vulnerability established in the eyes of our adversaries through a variety of deception mechanisms.

Now one may legitimately ask is this antiterrorism, counterterrorism, covert action or what ever? One of our problems is we create false dichotomies and bureaucratic definitions that constrain our thinking and reduce our operational effectiveness.

Basically, I see antiterrorism and counterterrorism as a continuum—offensive measures at one pole and defensive measures at the other. Depending on circumstances, an appropriate response may lie anywhere on that continuum and will likely be a mix of defensive and offensive measures that will shift in reaction to the moves and countermoves of the various parties as the situation plays out.

We have defined counterterrorism and antiterrorism as separate and distinct. The consequence is that we have ended up with two separate and distinct areas of expertise and, in turn, have created two separate and distinct communities that do not mesh as well as they should. We have, in effect, let definitions constrain our thinking, dictate our organizational structure and, at times, drive our operational response.

I would like to suggest consideration of a different organizational approach by creating a structure that is extremely fluid, flexible and, most importantly, threat driven. It would have both offensive and defensive capabilities and special teams, but all would be under a unified rubric. In essence, it would be a task force approach in which members, drawn from the Intelligence Community, would bring to the table specific skills needed to attack a particular terrorist group or issue. Once the problem is resolved, the team would disband and its members return to their home agencies. Should a new issue arise, a new tailored team would be fielded. It is much the approach we are using against bin Laden but, rather than being the exception, it would become the institutionalized norm.

Basically, I believe in a holistic approach in which one may pick and choose from an operational tool kit of offensive and defensive measures that enables us to tailor our response to a specific threat. And through covert action, deception, and a variety of psychological operations, we alter the perceptions of our adversary so he is led down a path to ultimate destruction. In the game of terrorist vs. antiterrorist, the clarity with which we view our enemy and ourselves will, to a large extent, determine the winners, the losers and the price paid by each.